A probabilistic algorithm to test local algebraic observability in polynomial time

Alexandre Sedoglavic
Laboratoire GAGE, École polytechnique
F-91128 Palaiseau, France
sedoglavic@gage.polytechnique.fr

Preliminary version* of February 1, 2008

Abstract

The following questions are often encountered in system and control theory. Given an algebraic model of a physical process, which variables can be, in theory, deduced from the input-output behavior of an experiment? How many of the remaining variables should we assume to be known in order to determine all the others? These questions are parts of the *local algebraic observability* problem which is concerned with the existence of a non trivial Lie subalgebra of the symmetries of the model letting the inputs and the outputs invariant.

We present a *probabilistic seminumerical* algorithm that proposes a solution to this problem in *polynomial time*. A bound for the necessary number of arithmetic operations on the rational field is presented. This bound is polynomial in the *complexity of evaluation* of the model and in the number of variables. Furthermore, we show that the *size* of the integers involved in the computations is polynomial in the number of variables and in the degree of the differential system.

Last, we estimate the probability of success of our algorithm and we present some benchmarks from our Maple implementation.

Keywords: Local algebraic observability, local algebraic identifiability, seminumerical algorithm.
Mathematics Subject Classification (2000): 93B07, 93B40, 93A30; 12H05.

1 Introduction, Notations and Main Result

Local algebraic observability is a structural property of a model and one of the key-concepts in control theory. Its earliest definition goes back to the work of R.E. Kalman for the linear case (see [21]) and a large literature is devoted to

*This paper is available at [38]. All comments are welcome.

figure 1: Model for circadian oscillations in the Drosophila period protein [17]

$$\left\{\begin{array}{rcl} \dot{M} & = & \frac{v_s {K_I}^4}{{K_I}^4+{P_N}^4} - \frac{v_m M}{K_m+M}, \\ \dot{P}_0 & = & k_s M - \frac{V_1 P_0}{K_1+P_0} + \frac{V_2 P_1}{K_2+P_1}, \\ \dot{P}_1 & = & \frac{V_1 P_0}{K_1+P_0} + \frac{V_4 P_2}{K_4+P_2} - P_1\Big(\frac{V_2}{K_2+P_1} + \frac{V_3}{K_3+P_1}\Big), \\ \dot{P}_2 & = & \frac{V_3 P_1}{K_3+P_1} - P_2\Big(\frac{V_4}{K_4+P_2} + k_1 + \frac{v_d}{K_d+P_2}\Big) + k_2 P_N, \\ \dot{P}_N & = & k_1 P_2 - k_2 P_N, \\ y & = & P_N. \end{array}\right.$$

this subject (see [18, 46, 41, 11] and the references therein). We base our work on the definition given by S. Diop & M. Fliess in [11] of the observability for the class of algebraic systems.

As in the example of figure 1, such a system is usually described by means of

- a vector field, which describes the evolution of *state variables* in function of *inputs* and of *parameters*;
- some *outputs* which are algebraic functions of these variables.

The definition of observability given in [11] relies on the theory of differential algebra founded by J.F. Ritt [34] and is based on the existence of algebraic relations between the state variables and the successive derivatives of the inputs and the outputs.

These relations can be considered as an obstruction to the existence of infinitely many trajectories of the state variables which are solutions of the vector field and fit the same specified input-output behavior. If there are only finitely many such trajectories, the state variables are said to be locally observable.

In order to illustrate this notion, let us consider the *local structural identifiability* problem which is a particular case of the observability problem. The question is to decide if some unknown *parameters* of a model are observable considering their parameters as a special kind of state variables Θ satisfying $\dot{\Theta} = 0$ (see [33, 44, 29, 26, 9]). If they are not observable, then infinitely many values of these parameters can fit the same observed data. Hence, if these parameters have a physical significance, it may be necessary to change the experimental protocol when possible. On the other hand, if the parameters are identifiable, various numerical approximation methods can be used for their estimation (see [39] and the references therein).

We consider the local algebraic observability problem under the computer algebra standpoint. The previous studies that enable to test observability mainly rely on characteristic set or standard bases computation [33, 29, 26, 4, 19] and their complexity is, at least, exponential in the number of variables and of parameters (see [14, 35]). Some other techniques, as the local state-space isomor-

phism approach [44] or the conversion between characteristic set w.r.t. different ranking [3], can also be used. The complexities of these methods are not known.

We present a probabilistic polynomial-time algorithm which computes the set of observable variables of a model and gives the number of non observable variables which should be assumed to be known in order to obtain an observable system. A Maple implementation is available at [38].

Example: Let us consider the use of our algorithm with a model for circadian oscillations in the Drosophila period protein [17]. This model is presented in figure 1; there are seventeen parameters and no input in it. After one minute of computation, our Maple implementation gives the following results:

- the variable M and the parameters $\{v_s, v_m, K_m, k_s\}$ are not observable. All the other parameters and variables are observable;
- if the non observable variable or only one of the non observable parameters are specified, all the variables and parameters of the resulting system are observable.

Our algorithm certifies that a variable is observable and the answer for a non observable one is probabilistic with high probability of success.These results allow us to focus our attention on just four of the seventeen original parameters. Thus, the search of an infinitesimal transformation which leaves the output y and the vector field invariant is simplified and we find a group of symmetries generated by $\{M, v_s, v_m, K_m, k_s\} \rightarrow \{\lambda M, \lambda v_s, \lambda v_m, \lambda K_m, k_s/\lambda\}$. Hence, there is an infinite number of possible values for non observable parameters which fit the same specified output y: this system is certainly unidentifiable.

1.1 Notations and Main Result

Hereafter, we consider a state-space representation with time invariant parameters defined by an algebraic system of the following kind:

$$\Sigma \quad \left\{ \begin{array}{rcll} \dot{\Theta} & = & 0, & \\ \dot{X} & = & F(X, \Theta, U), & (1.1) \\ Y & = & G(X, \Theta, U). & (1.2) \end{array} \right.$$

Big letters stand for vector-valued objects and we suppose that there are:

- ℓ parameters $\Theta := (\theta_1, \ldots, \theta_\ell)$
- n state variables $X := (x_1, \ldots, x_n)$;
- r input variables $U := (u_1, \ldots, u_r)$;
- m outputs variables $Y := (y_1, \ldots, y_m)$ with $m \leq n$.

The letter $\dot{X}$ stands for the derivatives of the state variables $(\dot{x}_1, \ldots, \dot{x}_n)$ and F (resp. G) represents n (resp. m) rational fractions in $\mathbb{Q}(X, \Theta, U)$ which are

denoted by $(f_1, \ldots, f_n)$ $\big($resp. $(g_1, \ldots, g_m)\big)$. The letter d (resp. h) represents a bound on the degree (resp. size of the coefficients) of the numerators and denominators of the f_i's and g_i's.

Hereafter, we use a common encoding where the expression $e := x^5$ is represented as a sequence of instructions: $t_1 := x, t_2 := {t_1}^2, t_3 := {t_2}^2, e := t_3 t_1$.

Hence, the system Σ is represented by a *straight-line program* without division which computes its numerators and denominators and requires L arithmetic operations (see Section 3.4 and § 4 in [6]).

The following theorem is the main result of this paper.

Theorem 1 *Let Σ be a differential system as described in Section 1.1. There exists a probabilistic algorithm which determines the set of observable variables of Σ and gives the number of non observable variables which should be assumed to be known in order to obtain an observable system.*

The arithmetic complexity of this algorithm is bounded by

$$\mathcal{O}\left(M(\nu)\Big(N(n+\ell)+(n+m)L\Big)+(n+\ell+1)N(n+\ell)\frac{m\nu}{n+\ell}\right)$$

with $M(\nu)$ $\big($resp. $N(\nu)\big)$ the cost of power series multiplication at order $\nu+1$ (resp. $\nu \times \nu$ matrix multiplication) where $\nu \leq n+\ell$.

Let μ be an arbitrary positive integer, D be $4(n+\ell)^2(n+m)d$ and

$$D' := \big(2\ln(n+\ell+r+1)+\ln \mu D\big)D + 4(n+\ell)^2\big((n+m)h+\ln 2nD\big).$$

If the computations are done modulo a prime number $p > 2D'\mu$ then the probability of a correct answer is at least $(1-1/\mu)^2$.

For the model presented in figure 1, the significant terms of our complexity statement are $L = 91, n = 5, \ell = 17, m = 1, d = 6, h = 1, \nu = n+\ell$. The choice of $\mu = 3000$ leads to a probability of success around .9993 and the computations are done modulo 10859887151. These computations take 10 seconds on a PC Pentium III (633 Mhz) provided by the UMS MEDICIS [42].

Outline of the paper: In the next section, we recall some basic definitions of differential algebra and the definition of algebraic observability used by S. Diop & M. Fliess in [11]. Furthermore, we describe the relationship between this framework and the approach of H. Pohjanpalo in [31]. Then, we present an algebraic jacobian matrix which is derived from the theory of Kähler differentials and used in the local algebraic observability test.

In the second part of this paper, we present some new results. In Section 3, we show how to compute some specializations of this matrix using power series expansion of the output and we estimate the related arithmetic complexity. Then, we study the behavior of the integers involved in the computations and we precise the probabilistic aspect. In conclusion, we present some benchmarks.

2 Differential Algebra and Observability

Differential algebra, founded by J.F. Ritt, is an appropriate framework for the definition of algebraic observability introduced by S. Diop & M. Fliess in [11]. For more details on differential algebra, we refer to [34] and [24]; nevertheless, we recall briefly some necessary notions.

2.1 Differential Algebraic setting

Let us denote by k a base field of characteristic zero. The differential algebra $k\{U\}$ is the k-algebra of multivariate polynomials defined by the infinite set of indeterminates $\{U^{(j)} | \forall j \in \mathbb{N}^\star\}$ and equipped with a derivation δ such that $\delta u^{(i)} = u^{(i+1)}$. Its differential fraction field is denoted by $k\langle U\rangle$.

Hypotheses: The inputs U and all their derivatives are assumed to be independent. Furthermore, we consider non singular solutions of Σ; thus, we assume that we work in an open set where the denominators present in Σ do not vanish. These hypotheses represent practically all the encountered systems.

2.2 Local Algebraic Observability

Following the interpretation due to M. Fliess of some algebraic control theory problems [13], we consider the differential field $\mathcal{K} := k\langle U\rangle(X, \Theta)$ equipped with the following formal Lie derivation:

$$\mathcal{L} := \frac{\partial}{\partial t} + \sum_{i=1}^{n} f_i \frac{\partial}{\partial x_i} + \sum_{j\in\mathbb{N}} \sum_{u\in U} u^{(j+1)} \frac{\partial}{\partial u^{(j)}}.$$

This derivation is associated with the vector field defined by the equations (1.1). Hereafter, we denote $(\mathcal{L}f_1, \ldots, \mathcal{L}f_n)$ by $\mathcal{L}F$ and $\underbrace{\mathcal{L} \circ \cdots \circ \mathcal{L}}_{j \text{ times}}$ by $\mathcal{L}^j$.

Hence, the outputs $G(X, \Theta, U)$ are denoted by Y and $Y^{(j)} = \mathcal{L}^j G(X, \Theta, U)$.

Definition 1 ([26, 11]) *An element z in $\mathcal{K}$ is locally algebraically observable with respect to inputs and outputs if it is algebraic over $k\langle U, Y\rangle$. Thus, the system Σ is locally observable if the field extension $k\langle U, Y\rangle \hookrightarrow \mathcal{K}$ is purely algebraic.*

Let us illustrate this definition with the following example:

$$\begin{cases} \dot{x}_3 &= \theta x_1, \\ \dot{x}_2 &= x_3/x_2, \\ \dot{x}_1 &= x_2/x_1, \\ y &= x_1. \end{cases}$$

By successive differentiations of the output, we obtain the following differential relations:

$$y - x_1, \quad y\dot{y} - x_2, \quad y\dot{y}(\dot{y}^2 + y\ddot{y}) - x_3$$
$$(\dot{y}^2 + y\ddot{y})^2 + y\dot{y}\big(3\dot{y}\ddot{y} + yy^{(3)}\big) - \theta y.$$

Thus, the parameter and the variables are observable according to Definition 1. Furthermore, as these algebraic relations define a unique solution, the parameter and the variables are said to be *globally* algebraically observable [26, 29, 9].

These relations depend generically of high order derivatives of the output and thus, they are not of a great practical interest for parameter estimation. As we focus our attention on local observability, we are going to avoid their computation.

Convention: We wish to test observability for the parameters Θ and/or state variables X. Thus, we present the algorithm in the most general case (observability of parameters and state variables) and we do not describe the restriction to one case or the other.

Definition 1 implies that local algebraic observability is related to the transcendence degree of the field extension $k\langle U, Y\rangle \hookrightarrow \mathcal{K}$. So, this property can be tested by a rank computation using Kähler differentials (see Section 2.4). As noticed in [11], this approach leads to a condition which is the formal counterpart of the R. Hermann & A. Krener rank condition in the differential geometric point of view [18].

Furthermore, the transcendence degree of the field extension $k\langle U, Y\rangle \hookrightarrow \mathcal{K}$ is the number of non observable variables which should be assumed to be known in order to obtain an observable system. Thus, Theorem 1 is based on the study of this field extension.

2.3 A Description of $k\langle U, Y\rangle \hookrightarrow \mathcal{K}$

Let us denote by $\Phi(X, \Theta, U, t)$ the formal power series with coefficients in $\mathcal{K}$ such that $\Phi(X, \Theta, U, 0) := X$ and $\dot{\Phi} = F(\Phi, \Theta, U)$, we have:

$$\Phi(X, \Theta, U, t) = X + \sum_{j \in \mathbb{N}^\star} \mathcal{L}^j F(X, \Theta, U)\ \frac{t^j}{j!}.$$

Furthermore, let us define the formal power series $Y(X, \Theta, U, t)$ with coefficients in $\mathcal{K}$ such that $Y(X, \Theta, U, t) := G\big(\Phi(X, \Theta, U, t), \Theta, U, t\big)$:

$$Y(X, \Theta, U, t) = G(X, \Theta, U) + \sum_{j \in \mathbb{N}^\star} \mathcal{L}^j G(X, \Theta, U)\ \frac{t^j}{j!}. \tag{2}$$

We recall that these expressions are vector-valued $\big(Y = (y_1, \ldots, y_m)\big)$.

In [31], H. Pohjanpalo already considers the coefficients of the power series $Y(X, \Theta, U, t)$ in order to test identifiability. In [11], the authors prove that a finite number of these coefficients are necessary to *describe* the field extension $k\langle U, Y\rangle \hookrightarrow \mathcal{K}$. But in these two papers the necessary order of derivation is not bounded.

This can be done using the differential algebra point of view (see § 4 in [35] for a general statement). The following proposition summarizes these results in a field extension framework.

Proposition 1 *The field $k\langle U,Y\rangle$ is isomorphic to $k\langle U\rangle\big(Y,\ldots,Y^{(n+\ell+1)}\big)$ and algebraic over $k\langle U\rangle\big(Y,\ldots,Y^{(n+\ell)}\big)$.*

Proof: The transcendence degree of $k\langle U\rangle \hookrightarrow \mathcal{K}$ is equal to $n+\ell$. Hence, the transcendence degree of $k\langle U\rangle \hookrightarrow k\langle U,Y\rangle$ is bounded by $n+\ell$. It means that, for $i=1,\ldots,m$, there is an algebraic relation $q_i\big(y_i,\ldots,{y_i}^{(n+\ell)}\big)=0$ and the derivative ${y_i}^{(n+\ell+1)}$ is a rational function of $y_i,\ldots,{y_i}^{(n+\ell)}$ with coefficients in $k\langle U\rangle$. This proves that $k\langle U,Y\rangle$ is isomorphic to $k\langle U\rangle\big(Y,\ldots,Y^{(n+\ell)}\big)$. ■

If there is more than a single output, the necessary order of derivation can be smaller than $n+\ell$ and it is denoted by ν. This index of differentiation is a natural measure of the complexity of our algorithm (see Section 3.4) and generically $\nu=(n+\ell)/m$. Hereafter, we take ν equal to $n+\ell$ as in Theorem 1.

In the above proof, following the hypotheses of Section 2.1, we assumed that the independent input variables U and all their derivatives were in the base field. Furthermore, we showed that we just need the first $n+\ell$ derivatives of the output equations. In order to simplify the presentation in the next section, we assume that the base field is $\bar{k}:=k\big(U,Y,\ldots,U^{(n+\ell)},Y^{(n+\ell)}\big)$.

We present now the properties of the module of Kähler differentials which are used to compute the transcendence degree of $\bar{k}\hookrightarrow\bar{k}(X,\Theta)$ in practice.

2.4 Rank Conditions

If $S\hookrightarrow T$ is a field extension, we use the notation $\Omega_{T/S}$ for the T-vector space which is the cokernel of the jacobian matrix $\partial(\mathcal{L}^iG)_{0\leq i\leq\nu}/\partial(X,\Theta)$ and $\mathrm{d}z$ stands for the image of $z\in T$ in this vector space (see § 16 in [12] for standard definition and [20] for construction in differential algebra). We recall the following result:

Theorem 2 (§ 16 in [12]) *Let us consider S a field of characteristic zero and T a finitely generated field extension of S. If $\{x_\lambda\}_{\lambda\in\Lambda}\subset T$ is a collection of elements, then $\{\mathrm{d}x_\lambda\}_{\lambda\in\Lambda}$ is a basis of $\Omega_{T/S}$ as a vector space over T iff the $\{x_\lambda\}_{\lambda\in\Lambda}$ form a transcendence basis of T over S.*

Our algorithm is based on the following straightforward consequences of this theorem.

Corollary 1 *If ϕ is the transcendence degree of the field extension $\bar{k}\hookrightarrow\bar{k}(X,\Theta)$ then we have the equality*

$$\phi=(n+\ell)-\mathrm{rank}_{\bar{k}(X,\Theta)}\Big(\partial\big(\mathcal{L}^iG\big)_{0\leq i\leq\nu}/\partial(X,\Theta)\Big).$$

Furthermore, If the rank of the jacobian submatrix $\partial(\mathcal{L}^jG)_{0\leq j\leq\nu}/\partial(X\backslash\{x_i\},\Theta)$ (resp. $\partial(\mathcal{L}^jG)_{0\leq j\leq\nu}/\partial(X,\Theta\backslash\{\theta_i\})$) is equal to $n+\ell-\phi$, then the transcendence degree of the field extension $\bar{k}\hookrightarrow\bar{k}(x_i)$ (resp. $\bar{k}\hookrightarrow\bar{k}(\theta_i)$) is equal to zero and the variable x_i (resp. the parameter θ_i) is observable.

The computation of ϕ is mainly based on the construction and the evaluations of a *straight-line program* which allows to compute the power series expansion of $Y(X, \Theta, U, t)$. We present the necessary notions in the next section.

2.5 Data Encoding and Complexity Model

The above results can be expressed considering a polynomial f as an element of a vector space; hereafter, we consider an algebraic expression as a function.

This classical point of view in numerical analysis is also used in computer algebra for complexity statements or practical algorithms (see [16, 45, 36, 37] and the references therein). We refer to Chapter 4 of [6] for more details about this model of computation.

Definition 2 *Let $A := \{a_1, \ldots, a_j\}$ be a finite set of variables. A straight-line program is a sequence of assignments $b_i \leftarrow b' \circ_i b''$ where $\circ_i \in \{+, -, \times, \div\}$ and where $\{b', b''\} \subset \bigcup_{j=1}^{i-1}\{b_j\} \cup A \cup k$. Its complexity of evaluation is measured by its length L, which is the number of its arithmetic operations. Hereafter, we use the abbreviation* SLP *for straight-line program.*

As a SLP representing a rational expression $f \in k(a_1, \ldots, a_j)$ is a program which computes the value of f from any values of the base field such that every division of the program is possible. Furthermore, it is possible to determine a SLP representing the gradient of f. The following constructive results allows us to handle these two aspects.

Theorem 3 (W. Baur & V. Strassen [1]) *Let us consider a* SLP *computing the value of a rational expression f in a point of the base field and let us denote by L_f its complexity of evaluation.*

One can construct a SLP *of length $5L_f$ which computes the value of* $\mathrm{grad}(f)$.

Furthermore, one can construct a SLP of length $4L_f$ which computes two polynomials f_1 and f_2 such that $f = f_1/f_2$.

Following our presentation, one can construct formally all the expressions introduced in Sections 2.3 and 2.4 with its favourite computer algebra system.

But, let us recall that, in order to compute the formal expressions $\mathcal{L}^\nu G$ and the associated jacobian matrix, one has to differentiate ν times the output equations (1.2). As explained in [22], the arithmetic complexity of computing multiple partial derivatives is likely exponential in ν. If the evaluation complexity of the output equations (1.2) is L, by Theorem 3, the computation of $\mathcal{L}^\nu G$ requires at least $(5m)^\nu L$ arithmetic operations.

Thus, this strategy cannot lead to a polynomial time algorithm.

The rank computations defined in the previous section are also cumbersome because they are mainly performed on the field $\bar{k}(X, \Theta)$. Nevertheless, in order to determine ϕ efficiently, the variables X, Θ and U can be specialized to some generic values in the jacobian matrix and so, its generic rank can be computed numerically with high probability of success (see Section 3.6).

Thus, the main problem is to avoid the formal computation of $(\mathcal{L}^i G)_{0\leq i\leq \nu}$. In fact, our strategy is to specialize a linearized system derived form Σ first and to recover the value of ϕ just using numerical computations on a finite field.

3 A Probabilistic Polynomial-Time Algorithm

In Section 3.1, we present the *linear variational system* derived from Σ which allows us to compute directly the jacobian matrix $\partial(\mathcal{L}^i G)_{0\leq i\leq \nu}/\partial(X,\Theta)$ with X, Θ and U specialized on some given values.

Then, we show how this matrix can be determined in polynomial time and we give an estimation of the arithmetic complexity of our algorithm.

The purpose of the Sections 3.5 and 3.6 is to study the growth of the integers involved in the computations and to estimate the probability of success of our algorithm.

3.1 Variational System Derived From Σ

As shown in Section 2.4, our goal is to compute the generic rank of the jacobian matrix $\partial(\mathcal{L}^i G)_{0\leq i\leq \nu}/\partial(X,\Theta)$. Using relation (2), we conclude that:

$$\frac{\partial(\mathcal{L}^j G)_{0\leq j\leq \nu}}{\partial(X,\Theta)} = \frac{\partial\big(\mathsf{coeffs}\big(Y(t)\big)\big)}{\partial(X,\Theta)} = \mathsf{coeffs}\left(\frac{\partial G}{\partial X}\frac{\partial \Phi}{\partial X}, \frac{\partial G}{\partial X}\frac{\partial \Phi}{\partial \Theta} + \frac{\partial G}{\partial \Theta}\right).$$

The above equalities leads to the following relation:

$$\frac{\partial(\mathcal{L}^j G)_{0\leq j\leq \nu}}{\partial(X,\Theta)} = \mathsf{coeffs}\left(\nabla Y\left(\Phi, \frac{\partial \Phi}{\partial X}, \frac{\partial \Phi}{\partial \Theta}\right), t^j, j = 0, \ldots, \nu\right), \tag{3}$$

where ∇Y denote the following $n \times (n+\ell)$ matrix represented by a SLP:

$$\nabla Y\big(\Phi, \Gamma, \Lambda, \Theta, U\big) := \left(\frac{\partial G}{\partial X}\Gamma, \frac{\partial G}{\partial X}\Lambda + \frac{\partial G}{\partial \Theta}\right)\big(\Phi, \Gamma, \Lambda, \Theta, U\big).$$

Hence, we have to determine the first $\nu = n + \ell$ terms of the power series expansion of $\Phi(X,\Theta,U,t)$, $\Gamma(X,\Theta,U,t) := \partial\Phi/\partial X$ and $\Lambda(X,\Theta,U,t) := \partial\Phi/\partial\Theta$.

Let us denote by $P(\dot{X}, X, \Theta, U) = 0$, the numerators of the rational relations $\dot{X} - F(X,\Theta,U) = 0$ and let us consider the following expressions:

$$\nabla P \begin{cases} P(\dot{X}, X, \Theta, U), & (4.1) \\ \frac{\partial P}{\partial \dot{X}}(X,\Theta,U)\dot{\Gamma} + \frac{\partial P}{\partial X}(\dot{X}, X, \Theta, U)\Gamma, & (4.2) \\ \frac{\partial P}{\partial \dot{X}}(X,\Theta,U)\dot{\Lambda} + \frac{\partial P}{\partial X}(\dot{X}, X, \Theta, U)\Lambda + \frac{\partial P}{\partial \Theta}(\dot{X}, X, \Theta, U). & (4.3) \end{cases} \tag{4}$$

The power series $\Phi(X,\Theta,U,t)$, $\Gamma(X,\Theta,U,t)$ and $\Lambda(X,\Theta,U,t)$ are solutions of the system of ordinary differential equations $\nabla P(\Phi,\Gamma,\Lambda,\Theta,U) = 0$ with initial conditions $\Gamma(X,\Theta,U,0) := \mathrm{Id}_{n\times n}$ and $\Lambda(X,\Theta,U,0) := 0_{n\times \ell}$.

Commentary: We have already noticed that one can compute symbolically the expression of the formal jacobian matrix $\partial(\mathcal{L}^i G)_{0\leq i\leq \nu}/\partial(X,\Theta)$. The rank computations described in Corollary 1 are sufficient to conclude.

Furthermore, if X, Θ and U are specialized on some random values, these computations can be performed numerically with high probability of success. We summarize this possible strategy in the upper horizontal and the right vertical arrow of the following diagram:

$$\begin{array}{ccc} \Sigma & \xrightarrow{\text{formal computation}} & \left(\frac{\partial(\mathcal{L}^i G)_{0\leq i\leq \nu}}{\partial(X,\Theta)}\right) \\ & & \Big\downarrow \left\{\begin{array}{lcl} X & \rightarrow & X_0 \in \mathbb{Z}^n, \\ \Theta & \rightarrow & \widetilde{\Theta} \in \mathbb{Z}^\ell, \\ U & \rightarrow & \widetilde{U} \in (\mathbb{Z}[t])^r. \end{array}\right. \\ \nabla P & \xrightarrow{\text{numerical computation on } \mathbb{Q}} & \left(\frac{\partial(\mathcal{L}^i G)_{0\leq i\leq \nu}}{\partial(X,\Theta)}\right)\big(X_0, \widetilde{\Theta}, \widetilde{U}\big) \end{array}$$

As the symbolic computation of the jacobian matrix is cumbersome, we specialize the parameters on some random integers $\widetilde{\Theta}$ and the inputs U on the power series $\widetilde{U}$ which are truncated at order $n+\ell+1$ with random integer coefficients. Then, we solve the associated system ∇P for some integer initial conditions X_0 and we compute the specialization $\partial(\mathcal{L}^i G)_{0\leq i\leq \nu}/\partial(X,\Theta)(X_0,\widetilde{\Theta})$ with ∇Y. This approach is summarized by the left vertical and the lower horizontal arrow. We present an algorithm which relies on this standpoint and we give in Section 3.6 its probability of success.

The hypothesis $\partial P/\partial \dot{X} \neq 0$ assumed in Section 2.1 ensures that the differential system $\nabla P\big(\Phi, \Gamma, \Lambda, \widetilde{\Theta}, \widetilde{U}\big) = 0$ admits an unique formal solution [10] which can be computed with the following Newton operator.

3.2 A Quadratic Newton Operator

The aim of this section is to present the Newton operator used in our algorithm. In [15, 5], the authors show that such an operator is quadratic. We sketch its construction and neglect the technical details for the sake of simplicity.

We recall that we work with vector-valued expressions. Thus, the expression (4.1) $\big($resp. (4.2), (4.3)$\big)$ represents a $n \times 1$ (resp. $n \times n,\ n \times \ell$) matrix.

The Theorem 3 allows to construct, from a SLP of length L which encodes Σ, another SLP of length $\mathcal{O}\big(N(n+\ell)+nL\big)$ which encodes the system ∇P. For some given series Φ, Γ and Λ, this SLP computes the following $n \times (1+n+\ell)$ matrix:

$$\left(\begin{array}{ccc} p_1(\dot{\Phi},\Phi,\widetilde{\Theta},\widetilde{U}) & \frac{\partial P}{\partial \dot{X}}(\Phi,\widetilde{\Theta},\widetilde{U})\dot{\Gamma} & \frac{\partial P}{\partial X}(\Phi,\widetilde{\Theta},\widetilde{U})\dot{\Lambda} \quad + \\ \vdots & + & \frac{\partial P}{\partial X}(\dot{\Phi},\Phi,\widetilde{\Theta},\widetilde{U})\Lambda + \\ p_n(\dot{\Phi},\Phi,\widetilde{\Theta},\widetilde{U}) & \frac{\partial P}{\partial \dot{X}}(\dot{\Phi},\Phi,\widetilde{\Theta},\widetilde{U})\Gamma & \frac{\partial P}{\partial \Theta}(\dot{\Phi},\Phi,\widetilde{\Theta},\widetilde{U}) \end{array}\right).$$

Let us represent $\Phi(X,\Theta,U,t)$ $\big($resp. $\Lambda(X,\Theta,U,t),\ \Gamma(X,\Theta,U,t)\big)$ mod t^{2^j} by Φ_j $\big($resp. $\Lambda_j,\ \Gamma_j\big)$ and denote the correction term:

$$\big(\Phi(X,\Theta,U,t)-\Phi_j,\Gamma(X,\Theta,U,t)-\Gamma_j,\Lambda(X,\Theta,U,t)-\Lambda_j\big) \bmod t^{2^{j+1}} \text{ by } E_{j+1}.$$

As usually, we construct our Newton operator from the Taylor series expansion of the function ∇P. This yields the following relations:

$$\nabla P\big(\Phi,\Gamma,\Lambda\big)(X,\Theta,U,t) = \nabla P\big(\Phi_j,\Gamma_j,\Lambda_j\big)+\frac{\partial\,\nabla P}{\partial(\dot X,\dot\Gamma,\dot\Lambda)}\dot E_{j+1}+\frac{\partial\,\nabla P}{\partial(X,\Gamma,\Lambda)}E_{j+1}+\ldots=0.$$

The remaining terms are of order in t greater than 2^{j+1}. Thus, they are not necessary for the computation of E_j.

Computational strategy: we consider Φ as a variable in the first column of ∇P and as a constant in the others. Thus, we have the following relations:

$$\frac{\partial\,\nabla P}{\partial(\dot X,\dot\Gamma,\dot\Lambda)}=\left(\frac{\partial P}{\partial\dot X},\frac{\partial P}{\partial\dot X},\frac{\partial P}{\partial\dot X}\right),\quad \frac{\partial\,\nabla P}{\partial(X,\Gamma,\Lambda)}=\left(\frac{\partial P}{\partial X},\frac{\partial P}{\partial X},\frac{\partial P}{\partial X}\right).$$

Consequence of our computational strategy: The above hypothesis induces a *shift* between the order of correct coefficients of Λ_j, Γ_j and Φ_j. In fact, Λ_j and Γ_j are correct modulo $t^{2^{j-1}}$. Thus, we need to stop the following operator with $j+1=\ln_2(n+\ell+1)$ and to repeat one more time the last resolution at the same order.

Newton operator: The above hypothesis leads to a Newton operator based on the resolution of the following system of linear ordinary differential equations:

$$\frac{\partial P}{\partial\dot X}\big(\Phi_j,\widetilde\Theta,\widetilde U\big)\dot E_{j+1}+\frac{\partial P}{\partial X}\big(\dot\Phi_j,\Phi_j,\widetilde\Theta,\widetilde U\big)E_{j+1}+\nabla P\big(\Phi_j,\Gamma_j,\Lambda_j,\widetilde\Theta,\widetilde U\big)=0 \bmod t^{2^{j+1}} \quad (5)$$

From the initial conditions $\Phi_0\in\mathbb{Z}^n$, $\Gamma_0:=\mathrm{Id}_{n\times n}$ and $\Lambda_0:=0_{n\times\ell}$, this system is solved iteratively for $j+1=1,\ldots,\ln_2(n+\ell+1)$ using the recurrence relations $\big(\Phi_{j+1},\Gamma_{j+1},\Lambda_{j+1}\big)=\big(\Phi_j,\Gamma_j,\Lambda_j\big)+E_{j+1}$.

The resolution of the linear ordinary differential system (5) relies on the method of integrating factors. First, we consider the Homogeneous system

$$\frac{\partial P}{\partial\dot X}\big(\Phi_j,\widetilde\Theta,\widetilde U\big)\dot W_j+\frac{\partial P}{\partial X}\big(\dot\Phi_j,\Phi_j,\widetilde\Theta,\widetilde U\big)W_j=0 \bmod t^{2^{j+1}}$$

where W_j denote a $n\times n$ unknown matrix which coefficients are series truncated at order 2^j. The main trick is common in power series manipulation, we consider matrices with coefficients in a series ring as series with coefficients in a matrix ring. For example, we have $A \bmod t^{2^{j+1}}=A_0+A_1t+\cdots+A_{2^j}t^{2^j}$ where the A_i's are matrices with coefficients in the rational field.

Thus, the product, the exponential and, if A_0 is invertible, the inverse of matrices with coefficients in a series ring can be computed at precision j with the classical Newton operator (see 4.7 in [23] and § 5.2 in [5] for more details).

figure 2: Local Algebraic Observability Test

Input : $\dot{X} - F(X, \Theta, U),\ Y - G(X, \Theta, U)$
Output : Succeed, a boolean

Preprocessing Construction of the SLP coding $\frac{\partial P}{\partial \dot{X}}, \frac{\partial P}{\partial X}, \frac{\partial P}{\partial \Theta}, \nabla P, \Phi_\Theta$.

Initialization Choice of a prime number;

$U \leftarrow$ Random Power Series mod $t^{n+\ell+1}$;
Succeed$\leftarrow$ true; Order$\leftarrow$ 1; $\Theta\leftarrow$ Random Integers;
$\Lambda \leftarrow 0_{n\times\ell}$; $\Gamma \leftarrow \mathrm{Id}_{n\times n}$; $X \leftarrow$ Random Integers;

while Order $\leq n + \ell + 1$ **do**

$W \leftarrow \mathsf{HomogeneousResolution}\left(\frac{\partial P}{\partial \dot{X}}(\Phi, \Theta)\, \dot{W} + \frac{\partial P}{\partial X}(\dot{X}, \Phi, \Theta)\, W = 0\right) \bmod t^{\mathrm{Order}}$;

$(\Phi, \Lambda, \Gamma) \leftarrow (\Phi, \Lambda, \Gamma) + \mathsf{ConstantsVariation}\Big(W, \nabla P\,(\Phi, \Gamma, \Lambda)\Big) \bmod t^{\mathrm{Order}}$;

Increase Order; (Order $\leftarrow$ 2 Order);

end while

JacobianMatrix $\leftarrow \mathsf{Coeffs}\big(\nabla Y\,(\Phi, \Gamma, \Lambda), t^j, j = 0, \ldots, n + \ell\big)$;

Test
if $n + \ell >$ Rank(JacobianMatrix)
then Succeed := false
end if

For example, if A_0 is invertible and B_j denotes the inverse of A at order t^{2^j}, we have $B_{j+1} = 2B_j - B_j A B_j$.

Furthermore, it is a basic fact from the theory of linear ordinary system that if $A\dot{W} + A'W = 0$ and A is invertible then $W = \exp\big(\int A^{-1}A'\big)$ is a matricial solution of this system. Hence, the above homogeneous system can be solved at precision j by a procedure called HomogeneousResolution in figure 2.

With the same tools, one can check that the following formal expression deduced from the formula for variation of constants

$$W^{-1} \int \left(W \left(\frac{\partial P}{\partial \dot{X}} \right)^{-1} \nabla P \right) (\Phi_j, \Gamma_j, \Lambda_j, \widetilde{\Theta}, \widetilde{U}) dt$$

is a solution of system (5). This expression can be computed at precision j by a procedure called ConstantsVariation in figure 2.

3.3 Algorithm

We summarize our algorithm in figure 2. This is a simplified presentation where the technical details are neglected.

A preprocessing is necessary to construct, from a SLP coding Σ, another SLP which encodes the associated linear variational system ∇P and the expressions used during its integration. This step relies mainly on Theorem 3.

The next part of the algorithm consists in the computation at order $n+\ell+1$ of the power series solution of ∇P. We recall that in one iteration, the number of correct coefficients is doubled (see Theorem 2 in [15]).

After the main loop, the procedure Coeffs evaluates the SLP ∇Y on the series Φ_j, Γ_j and Λ_j where $j = \ln_2(n+\ell+1)$; this furnishes the coefficients of the jacobian matrix (see Section 3.1).

Last, the rank computations described in Corollary 1 are performed to solve the local observability problem.

If there is more than one output variable, the evaluation of ∇Y and the rank computations which are necessary to determine ϕ can be done in the main loop: the computation can be stopped when the expected rank is reached or when the computed ranks become stationary. Thus, we can determine the order of derivation ν and avoid useless computations.

We now present a rough upper bound for the arithmetic complexity.

3.4 Arithmetic Complexity Estimation

Notations: Hereafter, let L denote the complexity of evaluation of the system Σ and let $M(j)$ represent the multiplication complexity of two series at order $j+1$. Using classical multiplication formula, we have $M(j) \in \mathcal{O}\big(j^2\big)$.

Furthermore, let $N(j)$ denotes the number of arithmetic operations sufficient for the multiplication of two square $j \times j$ matrices. Using classical algorithms, we have $N(n) \in \mathcal{O}\big(j^3\big)$.

Proposition 2 *The number of arithmetic operations on the base field used in the algorithm presented in Section 3.3 is bounded by*

$$\mathcal{O}\left(M(\nu)\Big(N(n+\ell)+(n+m)L\Big)+(n+\ell+1)N(n+\ell)\frac{m\nu}{n+\ell}\right)$$

Proof: From construction done in Section 3.1 and Theorem 3, we conclude that the complexity of evaluation of the SLP coding $\partial P/\partial(\dot{X}, X, \Theta), \nabla P$ and ∇Y is bounded by $\mathcal{O}\big(N(n+\ell)+(n+m)L\big)$. Hence, at each step, the number of arithmetic operations necessary to evaluate this SLP on power series truncated at order j, is bounded by $\mathcal{O}\big(M(j)(N(n+\ell)+(n+m)L)\big)$.

Furthermore, the determination of the first j terms of the solution series of a system of linear ODE (5) requires $\mathcal{O}\big(M(j)(N(n)+N(n+\ell))\big)$ arithmetic operations by the well-known method of integrating factors (see § 5.2 in [5] for more details). So, as $M(j)+M\big(\lfloor j/2\rfloor\big)+\cdots=\mathcal{O}\big(M(j)\big)$ and as our Newton operator is quadratic, the arithmetic complexity of the computations of the jacobian matrix $\partial(\mathcal{L}^i G)_{0\leq i\leq\nu}/\partial(X,\Theta)$ is bounded by $\mathcal{O}\big(M(\nu)\big(N(n+\ell)+(n+m)L\big)\big)$.

To conclude, we notice that the cost of a rank computation for a $i \times j$ matrix is $\mathcal{O}\big(N(i)j/i\big)$ if $i \leq j$ (see page 108 in [2]). The Corollary 1 describes the rank computations done at the end of the main loop of our algorithm. ■

Remark: The specialization of input variables on a randomly chosen polynomial of degree $n+\ell$ increases the evaluation complexity L of the system Σ but it does not change the general complexity of the algorithm. When the system is not observable we assume that the index ν is $n+\ell$ (see Definition 4 in [7]).

We have presented the complexity of our algorithm in term of arithmetic operations on $\mathbb{Q}$. Such an operation requires a time, roughly, proportional to the size of its operands. Using modular techniques, we control the growth of the integers involved in the computations. We estimate now an upper bound on these integers; this bound will be used in Section 3.6 in order to estimate the probability of success of our algorithm.

3.5 Growth of the Integers

The forthcoming estimations relies on the formal definition of the jacobian matrix $\partial(\mathcal{L}^i G)_{0\leq i\leq \nu}/\partial(X,\Theta)$ and are not dependent of the computations described in Section 3.1 and 3.2.

Let us introduce a measure for the size of a $(n+\ell+r)$-variate polynomial which influence the growth of the integers (see [8] for more details).

Definition 3 *Let $\mathcal{A}$ be a finite set of non zero integers. The (logarithmic)* height *of $\mathcal{A}$ is defined as $ht(\mathcal{A}) := \ln|\mathcal{A}|$ with $|\mathcal{A}| := \max\{|\alpha|+1, \alpha\in\mathcal{A}\}$.*

The height of a polynomial with integer coefficients is defined by the height of its set of coefficients.

We summarize in the following lemma some basic properties of height:

Lemma 1 *Let $p_1,\ldots,p_s$ be $(n+\ell+r)$-variate polynomials with integer coefficients, x an integer and ∂ a partial derivation ($\partial/\partial x$ for example).*

- $ht(\partial p) \leq ht(p) + \ln\deg p$;
- $ht(p(x)) \leq ht(x)\deg p + ht(p)$;
- $ht\big(\sum_{i=1}^{s} p_i\big) \leq \max_{i=1..s} ht(p_i) + \ln s$;
- $ht(p_1p_2) \leq ht(p_1) + ht(p_2) + \min\{\deg p_1, \deg p_2\}\ln(n+\ell+r+1)$.

We use the notations introduced in Section 1.1 and we denote by h (resp. d) the maximum height (resp. degree) of the numerator and of the denominator of the expression involving in system Σ.

Proposition 3 *Let h_0 be the maximum of heights of the integers X_0, $\widetilde{\Theta}$ and of the integer coefficients of $\widetilde{U}$.*

- $ht\big(\text{denom}\,\mathcal{L}^j G\,(X_0)\big) \leq (2j+1)(n+m)\Big(\big(2\ln(n+\ell+r+1)+h_0\big)d+h\Big)$;
- $ht\big(\text{numer}\,\mathcal{L}^j G(X_0)\big) \leq \begin{array}{c}(2j+1)(n+m)\big((2\ln(n+\ell+r+1)+h_0)d+h\big)\\ +(j+1)\ln 2n(n+m)d+(2j+1)\ln(2j+1).\end{array}$

Proof: As we are interested in an upper bound, we do not consider the reduced form of the fractions f_i and g_i involved in $\mathcal{L}g$ but we consider that all these fractions share the same denominator q. So, $\mathcal{L} = \big(\sum f_i\partial_i\big)/q$ and q is the common denominator of all g_i.

Thus, the degree of these non-reduced numerators and denominators is bounded by $(n+m)d$ and the height by $(n+m)\big(h + d\ln(n+\ell+r+1)\big)$. Let us notice that the denominator of $\mathcal{L}^j g$ is q^{2j+1}; these facts and Lemma 1 prove the first part of our proposition.

We prove the second part by induction; let us consider $(v_j)_{j\in\mathbb{N}}$ the sequence of polynomials defined by the numerator of g as initial condition v_0 and by the recurrence relation $v_{j+1} := \sum f_i\big(q\partial_i v_j - (2j+1)v_j\partial_i q\big)$. By construction, v_j is equal to the numerator of $\mathcal{L}^j g$. Thus, the degree of v_j is bounded by $(2j+1)(n+m)d - j$ and we obtain the following recurrence relation from Lemma 1:

$$ht(v_{j+1}) \leq 2(n+m)\big(2d\ln(n+\ell+r+1) + h\big) + ht(v_j) + \ln 2n(2j+1)(n+m)d.$$

This is sufficient to conclude. ■

Remark: the use of non-reduced fractions simplifies the previous proof but it increases the upper bound by a factor $(n+m)$ which is not significant in this presentation.

We have showed that the size of the coefficients of the final specialized jacobian matrix is mainly linear in the differentiation index ν. But some intermediate computations can require integers of bigger size. In order to construct a practical and efficient algorithm, we have to avoid this growth using modular techniques.

Almost all the operations used in our algorithm commute with the canonical homomorphism from $\mathbb{Q}$ to a finite field $\mathbb{F}_p$. But, when we choose a prime number p, we have to avoid the cancellation of $\partial P/\partial\dot{X} \bmod t$ and of the determinant of $\partial(\mathcal{L}^i G)_{0\leq i\leq\nu}/\partial(X,\Theta)$.

The cancellation of $\partial P/\partial\dot{X} \bmod t$ can be checked at the begining of our algorithm. Thus, the probabilistic aspects concern mainly the choice of specialization and of a prime number such that the determinant of $\partial(\mathcal{L}^i G)_{0\leq i\leq\nu}/\partial(X,\Theta)$ does not vanish modulo p if this matrix is of full generic rank.

3.6 Probabilistic Aspects

Hereafter, we call a *bad point*, a set of specializations $\{X_0, \widetilde{\Theta}, \widetilde{U}\}$ where the jacobian matrix $\partial(\mathcal{L}^i G)_{0\leq i\leq\nu}/\partial(X,\Theta)$ is not of full generic rank. Thus, a bad point is a zero of the polynomial associated with a minor of this matrix. We estimate the probability for a specializations to be a bad point with the following proposition.

Proposition 4 (R. Zippel & J. Schwartz [47]) *Let q be a s-variate polynomial of total degree D and Ω a set of integers. The worst case bound for the probability that a point in Ω^s will be a zero of q is $D/\#\Omega$.*

This result shows the relation between the choice of the size h_0 of the used specializations and the probability of success of our algorithm. In fact, as the determinant of $\partial(\mathcal{L}^i G)_{0\leq i\leq \nu}/\partial(X,\Theta)$ is a polynomial of degree bounded by $D := (n+\ell)(2\nu+1)(n+m)d$, a point in $\{0,\ldots,\mu_1 D\}^{(n+\ell)(r+1)}$ is not a bad point with probability at least $1-1/\mu_1$.

Furthermore, we can estimate the probability that the determinant is divisible by a prime number p with the following arithmetic analogue of Proposition 4.

Proposition 5 (§ 18 in [45]) *For any integers a and b such that $b<a<c$, the probability that a prime number p between $b+1$ and $2b$ divides a is bounded by $2\ln c/b$.*

From Proposition 3 and Lemma 1, we can estimate the size of the coefficients of the specialization of the jacobian matrix $\partial(\mathcal{L}^i G)_{0\leq i\leq \nu}/\partial(X,\Theta)$. Thus, using Hadamard's inequality, we find the following rough upper bound for the size of the specialized determinant:

$$ht(c) := \big(2\ln(n+\ell+r+1)+h_0\big)D + (n+\ell)(2\nu+1)\big((n+m)h+\ln 2nD\big)$$

Thus, if the computations are performed modulo a prime number p greater or equal to $2ht(c)\,\mu_2$ then the probability that the specialized determinant is not divisible by p is at least $1-1/\mu_2$. These results lead to the following estimation.

Proposition 6 *Let μ be an arbitrary positive integer and*

$$\begin{array}{rcl} D & := & (n+\ell)(2\nu+1)(n+m)d, \\ ht(c) & := & \big(2\ln(n+\ell+r+1)+\ln D\big)D + (n+\ell)(2\nu+1)\big((n+m)h+\ln 2nD\big). \end{array}$$

If the matrix $\partial(\mathcal{L}^i G)_{0\leq i\leq \nu}/\partial(X,\Theta)$ is of full generic rank then the determinant of this matrix specialized on random integers in $\{0,\ldots,\mu D\}$ is not divisible by a prime number $p>2ht(c)\,\mu$ with probability at least $(1-1/\mu)^2$.

4 Experimental Results

We present now some benchmarks from an implementation in Maple [38] of our algorithm. The Maple computer algebra system provides almost all the necessary tools to handle the canonical isomorphism between polynomials and polynomial functions: this explains why we have chosen it to implement our algorithm.

The computations summarized in figure 3 have been performed on a personal computer Pentium III (633 Mhz) with 128Mb of memory running Linux 2.2 and Maple V.5. This computer was provided by the UMS MEDICIS [42].

These results show that the index of differentiation is a significant characteristic of the complexity of algorithm presented in Section 3.3. Furthermore, the last example of the array shows that the complexity of evaluation have a significative influence and that the total number of multiplications is clearly less significant than the number of multiplications between state and input variables.

figure 3: Some benchmarks

System	m	ν	ℓ	n	r	L	time in s.
V1987	2	8	5	4		17	0.8
R1986	2	14	9	4	1	19	1.5
MV1991	2	14	8	5	2	59	2.4
MW2000	3	18	14	4		67	5.7
KD1999	2	19	14	5	2	34	6.
G1995	1	23	17	5		46	10.
SHH1997	1	23	13	9		38	13.5

4.1 Certifying the result

As shown in Corollary 1, the local observability property is associated to the fact that the jacobian matrix is of full rank. Our algorithm computes the generic rank of this matrix. When it is maximal, the result is certainly correct. Hence, if this algorithm states that a model is observable then this result is certified (it is a RP-complexity class test, see § 25.8 in [45]).

If there is a non empty set $O \subset X \cup \Theta$ of non observable variables and parameters, the observable parameters can be randomly specialized and there is an infinitesimal transformation acting on the non observable state variables and parameters,

$$\mathcal{S} := \sum_{x \in O \cap X} s_x \frac{\partial}{\partial x} + \sum_{\theta \in O \cap \Theta} s_\theta \frac{\partial}{\partial \theta},$$

which leaves invariant the outputs G and the vector field associated to the model. This leads to the following linear system of PDE's:

$$\begin{cases} [\mathcal{S}, \mathcal{L}] & = 0, \\ \mathcal{S}G & = 0. \end{cases}$$

This system of PDE can be difficult to solve; nevertheless, we are not interested in the whole Lie algebra but in any non trivial subalgebra which can certified our result.

Furthermore, our algorithm decreases the number of unknown of the original problem. Hence, in many cases of practical interest, there is a rather straightforward solution (compare with [30]). For example, these computations have been performed in less than a hour with Maple for the following examples.

4.2 Examples

We present now the examples indicated in figure 3, the answer of our algorithm and some results of the method sketched in section 4.1. We just give the non observable parameters and variables; the other one are observable.

V1987 Model of a flow reactor to pyrolyze methane

This example is taken from [43].

$$\left\{\begin{array}{lcl} \dot{x}_1 &=& -x_1(k_1+k_2x_4)+k_5x_3x_4,\\ \dot{x}_2 &=& k_2x_1x_4-(k_3+k_4)x_2,\\ \dot{x}_3 &=& k_4x_2-k_5x_3x_4,\\ \dot{x}_4 &=& x_1(k_1+k_2x_4)+2k_3x_2-k_5x_3x_4,\\ y_1 &=& x_1,\\ y_2 &=& x_2. \end{array}\right.$$

Our Maple implementation certifies that all the variables and the parameters are observable.

R1986 A pharmacokinetic model

This example is taken from [32]. The letter u denotes an input.

$$\left\{\begin{array}{lcl} \dot{x}_1 &=& u-(c_1+c_2)x_1,\\ \dot{x}_2 &=& c_1x_1-(c_3+c_6+c_7)x_2+c_5x_4,\\ \dot{x}_3 &=& c_2x_1+c_3x_2-c_4x_3,\\ \dot{x}_4 &=& c_6x_2-c_5x_4,\\ y_1 &=& c_8x_3,\\ y_2 &=& c_9x_2. \end{array}\right.$$

Our Maple implementation gives the following results:

- the variables $\{x_2, x_3, x_4\}$ and the parameters $\{c_1, c_2, c_3, c_7, c_8, c_9\}$ are not observable;
- the transcendence degree of the field extension $k\langle U, Y\rangle \hookrightarrow \mathcal{K}$ is 1.

Further computations show that the following one parameter group

$$\begin{array}{lcc} x_2 &\to& \lambda x_2\\ x_3 &\to& ((1-\lambda)c_1+c_2)x_3/c_2\\ x_4 &\to& \lambda x_4\\ c_1 &\to& \lambda c_1\\ c_2 &\to& (1-\lambda)c_1+c_2 \end{array} \qquad \begin{array}{lcc} c_3 &\to& \big((1-\lambda)c_1+c_2\big)c_3/\lambda c_2\\ c_7 &\to& c_7-c_3(c_1+c_2)(1-\lambda)/\lambda c_2\\ c_8 &\to& -c_8c_2/\big((1-\lambda)c_1+c_2\big)\\ c_9 &\to& c_9/\lambda \end{array}$$

is composed of symmetries which leave the vector field and the output invariant.

MV1991 Model for an induction motor

This example is taken from [28]. The letters u_x and u_y denote inputs.

$$\left\{\begin{array}{rcl} \sigma & = & L_s - \frac{M^2}{L_r}, \qquad \gamma_N \;=\; \frac{M^2 R_r + {L_r}^2 R_s}{\sigma {L_r}^2}, \\ \\ \dot{\omega} & = & \frac{n_p M}{J L_r}(\Psi_x I_y - \Psi_y I_x) - \frac{T_L}{J}, \\ \dot{\Psi}_x & = & -\frac{R_r}{L_r}\Psi_x - n_p \omega \Psi_y + \frac{R_r}{L_r} M I_x, \\ \dot{\Psi}_y & = & n_p \omega \Psi_x - \frac{R_r}{L_r}\Psi_y + \frac{R_r}{L_r} M I_y, \\ \dot{I}_x & = & \frac{M R_r}{\sigma {L_r}^2}\Psi_x + \frac{n_p M}{\sigma L_r}\omega \Psi_y - \gamma_N I_x + \frac{u_x}{\sigma}, \\ \dot{I}_y & = & -\frac{n_p M}{\sigma L_r}\omega \Psi_x + \frac{M R_r}{\sigma {L_r}^2}\Psi_y - \gamma_N I_y + \frac{u_y}{\sigma}, \\ \\ y_1 & = & \omega, \\ y_2 & = & {\Psi_x}^2 + {\Psi_y}^2. \end{array}\right.$$

Our Maple implementation gives the following results:

- the variables $\{I_x, I_y\}$ and the parameters $\{M, L_s, R_s, L_r, R_r, J, T_l\}$ are not observable;
- the transcendence degree of the field extension $k\langle U, Y\rangle \hookrightarrow \mathcal{K}$ is 1.

Further computations show that the following one parameter group

$$\{I_x, I_y, M, L_s, R_s, L_r, R_r, J, T_l\} \to \{\lambda I_x, \lambda I_y, M\lambda, L_s\lambda, R_s\lambda, L_r/\lambda, \lambda R_r, \lambda J, \lambda T_l\}$$

is composed of symmetries which leave the vector field and the output invariant.

MW2000 Multispecies model for the transmission of pathogens

This example is taken from [27].

$$\left\{\begin{array}{rcl} b & = & \mu + c_1(y_1 + y_{12}), \\ \lambda_1 & = & \beta_1(y_1 + y_{12}), \\ \lambda_2 & = & \beta_2(y_2 + y_{12}) + I_2, \\ \\ \dot{x}_{12} & = & (1 - \theta_1 - \theta_2)b - (m_1\lambda_1 + m_2\lambda_2 + \mu)x_{12} + \\ & & (\nu_1 + \tau)y_1 + (\nu_2 + \tau)y_2 + \tau y_{12}, \\ \dot{y}_1 & = & \theta_1 b + m_1\lambda_1 x_{12} + \nu_2 y_{12} - \big((1 - \pi_2)m_2\lambda_2 + \nu_1 + \mu + c_1 + \tau\big)y_1, \\ \dot{y}_2 & = & \theta_2 b + m_2\lambda_2 x_{12} + \nu_1 y_{12} - \big((1 - \pi_1)m_1\lambda_1 + \nu_2 + \mu + \tau\big)y_2, \\ \dot{y}_{12} & = & (1 - \pi_1)m_1\lambda_1 y_2 + (1 - \pi_2)m_2\lambda_2 y_1 - (\nu_1 + \nu_2 + \mu + c_1 + \tau)y_{12}, \\ \\ o_1 & = & x_{12} + y_1 + y_2 + y_{12}, \\ o_2 & = & y_1 + y_{12}, \\ o_3 & = & y_2 + y_{12}. \end{array}\right.$$

Our Maple implementation gives the following results:

- with the exception of $\{\beta_1, \beta_2, I_2, m_1, m_2\}$, all the parameters are observable;
- the transcendence degree of the field extension $k\langle U, Y\rangle \hookrightarrow \mathcal{K}$ is 2.

Further computations show that the following two parameters group

$$\{\beta_1,\ \beta_2,\ I_2,\ m_1,\ m_2\} \to \{\beta_1/l_1,\ \beta_2/l_2,\ I_2/l_2,\ l_1 m_1,\ l_2 m_2\}$$

is composed of symmetries which leave the vector field and the output invariant.

Let us notice that the output o_1 is in fact a constraint equal to 1. Hence, our model can be composed of relations of order zero which can be considered as supplementary outputs.

KD1999 Model for a chemical reactor

This example is taken from [25].

$$\left\{\begin{array}{lcl} \dot{C}_A &=& \frac{F_A}{V}(C_{A0} - C_A) - k_0 e^{-E/RT} C_A, \\ \dot{C}_B &=& -\frac{F_A}{V} C_B) + k_0 e^{-E/RT} C_A, \\ \dot{T} &=& \frac{F_A}{V}(T_A - T) - k_0 e^{-E/RT} C_A \frac{\Delta H_r}{\rho c_p} + \frac{U}{\rho c_p}\frac{T_j - T}{V}, \\ \dot{T}_j &=& \frac{F_h}{V_h}(T_h - T_j) - \frac{U}{\rho_h c_{ph}}\frac{T_j - T}{V_h}, \\ y_1 &=& C_B, \\ y_2 &=& T. \end{array}\right.$$

We denote by A the Arrhenius' law $e^{-E/RT}$ and we add the ordinary differential equation $\dot{A} = EA\dot{T}/(RT^2)$ to the model. Our Maple implementation gives the following results:

- the variable A and the parameters $\{E, R, \Delta H_r, U, \rho, c_p, \rho_h, c_{ph}, k_0\}$ are not observable;
- the transcendence degree of the field extension $k\langle U, Y\rangle \hookrightarrow \mathcal{K}$ is 5.

Further computations show that the following five parameters group

$$\begin{array}{lcl} A &\to& \lambda_1 A \\ k_0 &\to& k_0/\lambda_1 \\ E &\to& \lambda_2 E \\ R &\to& \lambda_2 R \end{array} \qquad \begin{array}{lcl} \rho &\to& \lambda_3 \rho \\ c_p &\to& \lambda_4 c_p \\ \Delta H_r &\to& \lambda_3\lambda_4 \Delta H_r \end{array} \qquad \begin{array}{lcl} U &\to& \lambda_3\lambda_4 U \\ c_{ph} &\to& \lambda_5 c_{ph} \\ \rho_h &\to& \lambda_3\lambda_4\rho_h/\lambda_5 \end{array}$$

is composed of symmetries which leave the vector field and the output invariant.

G1995 Model of Circadian oscillations in the Drosophila period protein

This example is described in introduction.

SHH1997 Model of a part of the blood coagulation mechanism

This example is taken from [40].

$$
\begin{array}{lll}
r_1 = \frac{kc_X X \cdot RVV}{km_X + X}, & r_2 = ki_{Xa} Xa, & r_3 = \frac{kc_V V \cdot IIa}{km_V + V}, \\
r_4 = k_{PT} Va \cdot Xa \cdot PL, & r_5 = k_{PL} PT, & r_6 = \frac{kc_{II} \cdot II \cdot PT}{km_{II} + II}, \\
r_7 = \frac{kc_2 II \cdot Xa}{km_2 + II}, & r_8 = ki_{IIa\alpha_2 M} \cdot IIa, & r_9 = ki_{IIaATIII} \cdot IIa.
\end{array}
$$

$$
\left\{
\begin{array}{rcl}
\dot{X} & = & -r_1, \\
\dot{Xa} & = & r_1 - r_2 - r_4 + r_5, \\
\dot{V} & = & -r_3, \\
\dot{Va} & = & r_3 - r_4 + r_5, \\
\dot{PL} & = & -r_4 + r_5, \\
\dot{PT} & = & r_4 - r_5, \\
\dot{II} & = & -r_6 - r_7, \\
\dot{IIa} & = & r_6 + r_7 - r_8 - r_9, \\
\dot{IIa\alpha_2 M} & = & r_9, \\
y & = & IIa + \frac{556}{1000} IIa\alpha_2 M.
\end{array}
\right.
$$

Our Maple implementation gives the following results:

- the parameters $\{kc_X, km_X, kc_V, km_V, k_{PT}, kc_{II}, kc_2\}$ and the variables $\{X, Xa, V, Va, PL, PT\}$ are not observable;
- the transcendence degree of the field extension $k\langle U, Y\rangle \hookrightarrow \mathcal{K}$ is 1.

Further computations show that the following one parameter group

$$
\begin{array}{lcl@{\qquad}lcl@{\qquad}lcl}
X & \to & \lambda X & PL & \to & \lambda PL & kc_V & \to & \lambda kc_V \\
Xa & \to & \lambda Xa & PT & \to & \lambda PT & km_V & \to & \lambda km_V \\
V & \to & \lambda V & kc_X & \to & \lambda kc_X & k_{PT} & \to & k_{PT}/\lambda^2 \\
Va & \to & \lambda Va & km_X & \to & \lambda km_X & kc_{II} & \to & kc_{II}/\lambda \\
 & & & & & & kc_2 & \to & kc_2/\lambda
\end{array}
$$

is composed of symmetries which leave the vector field and the output invariant.

Acknowledgment: It is a pleasure to thank M. Giusti, G. Lecerf, F. Ollivier and É. Schost for their contributions, helpful comments and illuminating discussions.

References

[1] Baur, W., and Strassen, V. The complexity of partial derivatives. *Theoretical Computer Science 22* (1983), 317–330.

[2] Bini, D., and Pan, V. *Polynomial and matrix computations.* No. 12 in Progress in Theoretical Computer Science. Birkhäuser, 1994.

[3] Boulier, F. Efficient computation of regular differential systems by change of rankings using Kähler differentials. Preprint LIFL 1999-14, Dec. 1999.

[4] Boulier, F., Lazard, D., Ollivier, F., and Petitot, M. Representation for the radical of a finitely generated differential ideal. In *Proceedings of the 1995 International Symposium on Symbolic and Algebraic Computation* (Montreal, Canada, July 10–12 1995), A. H. M. Levelt, Ed., ACM, ACM Press, pp. 158–166.

[5] Brent, R. P., and Kung, H. T. Fast algorithms for manipulating formal power series. *Journal of the Association for Computing Machinery 25*, 4 (Oct. 1978), 581–595.

[6] Bürgisser, P., Clausen, M., and Shokrollahi, M. A. *Algebraic Complexity Theory*, vol. 315 of *Grundlehren der Mathematischen Wissenschaften*. Springer, 1997.

[7] Campbell, S. L., and Gear, C. W. The index of general nonlinear DAE's. *Numerische Mathematik 72* (1995), 173–196.

[8] Castro, D., Hägele, K., Morais, J., and Pardo, L. M. Kronecker's and Newton's approaches to solving: a first comparaison. *To appear in Journal of Complexity* (1999). Available at http://tera.medicis.polytechnique.fr/.

[9] Chappell, M. J., Godfrey, K. R., and Vajda, S. Global identifiability of the parameters of nonlinear systems with specified inputs: A comparison of methods. *Mathematical Biosciences 102* (1990), 41–73.

[10] Denef, J., and Lipshitz, L. Power series solutions of algebraic differential equations. *Mathematische Annalen 267* (1984), 213–238.

[11] Diop, S., and Fliess, M. On nonlinear observability. In *Proceedings of First European Control Conference* (Grenoble, France, July 2–5 1991), C. Commault and coll., Eds., vol. 1, Hermès, pp. 152–157.

[12] Eisenbud, D. *Commutative Algebra with a View Toward Algebraic Geometry*. No. 150 in Graduate Texts in Mathematics. Springer, 1994.

[13] Fliess, M. Automatique et corps différentiels. *Forum Mathematicum 1* (1989), 227–238.

[14] Gallo, G., and Mishra, B. Efficient algorithms and bounds for Wu-Ritt characteristic sets. In *Effective methods in algebraic geometry (proceedings of MEGA'90)* (Livorno, Italy, Apr. 17–21 1991), F. Mora and C. Traverso, Eds., vol. 94 of *Progress in Mathematics*, Birkhäuser, pp. 119–142.

[15] Geddes, K. Convergence behaviour of the Newton iteration for first order differential equations. In *Symbolic and Algebraic Computation, Proceedings of EUROSAM'79* (Marseille, France, June 1979), E. W. Ng, Ed., no. 72 in LNCS, Springer-Verlag, pp. 189–199.

[16] Giusti, M., Lecerf, G., and Salvy, B. A Gröbner free alternative for polynomial systems solving. Preprint 99–04, GAGE laboratory, available at http://www.gage.polytechnique.fr/notes/, 1999. To appear in Journal of Complexity in the proceedings of FoCM'99.

[17] Goldbeter, A. A model for circadian oscillations in the Drosophila period protein. *Proceedings of the Royal Society London B*, 261 (1995), 319–324.

[18] Hermann, R., and Krener, A. Nonlinear controllability and observability. *IEEE Transactions on Automatic Control AC-22* (1977), 728–740.

[19] Hubert, É. Factorisation free decomposition algorithms in differential algebra. *Journal of Symbolic Computation 29*, 4 & 5 (Apr./May 2000), 641–662.

[20] Johnson, J. Kähler differentials and differential algebra. *Annals of Mathematics 89* (1969), 92–98.

[21] Kalman, R. On the general theory of control systems. In *Proceedings of the first international congress on automatic control* (Moscow, SSSR, 1961), vol. 1, Butterworths, London, pp. 481–492.

[22] Kaltofen, E. Computational differentiation and algebraic complexity theory. In *Workshop Report on First Theory Institute on Computational Differentiation* (Argonne, Illinois, Dec. 1993), C. H. Bischo, A. Griewank, and P. M. Khademi, Eds., pp. 28–30. vol. ANL/MCS-TM-183 of Tech. Rep. Argonne National Laboratory.

[23] Knuth, D. E. *The Art of Computer Programming, Seminumerical Algorithms*, third ed., vol. 2. Addison-Wesley, 1998.

[24] Kolchin, E. R. *Differential Algebra and Algebraic Groups*. Academic Press, New-York, 1973.

[25] Kumar, A., and Daoutidis, P. *Control of nonlinear differential algebraic equation systems*. No. 397 in Research Notes in Mathematics. Chapman and Hall / CRC, 1999.

[26] Ljung, L., and Glad, T. Parametrization of nonlinear model structures as linear regressions. In *11th IFAC Word Congress* (Tellin, Estonia, Aug. 1990), pp. 67–71.

[27] Margaria, G., and White, L. Multispecies model for the transmission of pathogens. Private communication.

[28] Marino, R., and Valigi, P. Nonlinear control of induction motors: a simulation study. In *Proceedings of First European Control Conference* (Grenoble, France, July 2–5 1991), C. Commault and coll., Eds., vol. 1, Hermès, pp. 1057–1062.

[29] Ollivier, F. *Le problème de l'identifiabilité structurelle globale: approche théorique, méthodes effectives et bornes de complexité*. PhD thesis, École polytechnique, June 1990.

[30] Ollivier, F. Identifiabilité et identification : du calcul formel au calcul numérique ? In *Automatique, Biologie et Santé : modélisation et commande de régulations biologiques* (Paris, France, May 2000), vol. 9 of *European Series in Applied and Industrial Mathematics*, EDP Sciences–SMAI, pp. 93–99. Available at http://www.emath.fr/Maths/Proc/.

[31] Pohjanpalo, H. System identifiability based on the power series expansion of the solution. *Mathematical Biosciences 41* (1978), 21–33.

[32] Raksanyi, A. *Utilisation du calcul formel pour l'étude des systèmes d'équations polynomiales (applications en modélisation)*. PhD thesis, Université Paris-Dauphine, 1986.

[33] Raksanyi, A., Lecourtier, Y., Walter, É., and Venot, A. Identifiability and distinguishbility testing via computer algebra. *Mathematical Biosciences 77* (1985), 245–266.

[34] Ritt, J. F. *Differential Algebra*. Dover Publications, 1966.

[35] Sadik, B. A bound for the order of characteristic set elements of an ordinary prime differential ideal and some applications. *Applicable Algebra in Engineering Communications and Computing 10*, 3 (Mar. 2000), 251–268.

[36] Schost, É. Computing parametric geometric resolutions. Manuscript 2000-03, GAGE laboratory, Available at http://www.gage.polytechnique.fr/notes/, Jan. 2000.

[37] Sedoglavic, A. A mixed symbolic-numeric method to study prime ordinary differential ideal. Manuscript 2000-04, GAGE laboratory, available at http://www.gage.polytechnique.fr/notes/, Jan. 2000.

[38] Sedoglavic, A. Personal home page, http://medicis.polytechnique.fr/~sedoglav, valid August 2000.

[39] Stortelder, W. Parameter estimation in chemical engineering; a case study for resin production. Tech. Rep. NM-R9610, Centrum voor Wiskunde en Informatica, available at http://www.cwi.nl/, 1996.

[40] Stortelder, W. J. H., Hemker, P. W., and Hemker, H. C. Mathematical modelling in blood coagulation; simulation and parameter estimation. Tech. Rep. MAS-R9720, Centrum voor Wiskunde en Informatica, available at http://www.cwi.nl/, Sept. 30 1997.

[41] Sussmann, H. J. Single-input observability of continuous-time systems. *Mathematical System Theory 12* (1979), 371–393.

[42] UMS MEDICIS 658. http://www.medicis.polytechnique.fr/. CNRS–École polytechnique (Palaiseau, France), valid August 2000.

[43] Vajda, S. Identifiability of polynomial systems: structural and numerical aspect. In *Identifiability of parametric models* (1987), É. Walter, Ed., Pergamon Press, pp. 42–48.

[44] Vajda, S., Godfrey, K. R., and Rabitz, H. Similarity transformation approach to identifiability analysis of non linear comportemental models. *Mathematical Biosciences 93* (1989), 217–248.

[45] von zur Gathen, J., and Gerhard, J. *Modern Computer Algebra*. Cambridge university press, 1999.

[46] Williamson, D. Observation of bilinear systems with application to biological control. *Automatica 13* (1977), 243–254.

[47] Zippel, R. *Effective Polynomial Computation*. Kluwer Academic Publishers, 1993.